

13/12/2011

www.enisa.europa.eu

Clarifier les déclarations des incidents de cyber-sécurité : directives pour appliquer la nouvelle réglementation des télécommunications sur la sécurité et l'intégrité «Article 13a»

L'ENISA, l'agence de cyber-sécurité de l'UE, a annoncé aujourd'hui la publication de deux directives techniques. La première décrit comment appliquer le plan de déclaration obligatoire des incidents de cyber-sécurité pour les opérateurs de télécommunication, les paramètres et les seuils, et les méthodes de déclaration; la seconde décrit des mesures de sécurité spécifiques qui devraient être prises par les opérateurs de télécommunication.

La nouvelle réglementation relative aux télécommunications (directive de l'UE 2009/140/EC) protège [entre autres](#) les consommateurs contre les violations de la sécurité. L'Article 13a de cette nouvelle réglementation demande aux opérateurs de télécommunication de signaler les incidents de sécurité et de prendre des mesures de sécurité pour assurer une provision des services de communication sécurisée et ininterrompue sur l'ensemble des réseaux de télécommunications européens.

En 2010, l'ENISA, la Commission Européenne (CE), les ministères des États-membres et les Autorités nationales de réglementation des télécommunications (NRA), tel que le prévoyait l'«Art. 13 Groupe de travail», ont collaboré dans le but de clarifier les modalités de déclaration et de garantir une application cohérente de l'Article 13a. Ce groupe d'acteurs est parvenu à un consensus sur deux directives : **Directive technique sur la déclaration des incidents de cyber-sécurité** et **Directive technique sur la mise en place de mesures de sécurité minimales**.

«Les précisions indiquant comment déclarer les incidents de cyber-sécurité et comment appliquer l'article 13a de manière cohérente fournissent des conditions de concurrence égales pour le secteur européen des télécommunications. Cela éliminera les barrières pour les fournisseurs européens de télécommunication au-delà des frontières», ont affirmé Dimitra Liveri et Marnix Dekker, rédacteurs des deux documents.

«La déclaration des incidents et les mesures de sécurité minimales sont des outils importants pour renforcer la confiance des clients, des entreprises et des gouvernements dans la sécurité des services de télécommunication. Après la récente affaire [Diginotar](#), on assiste à une augmentation du soutien pour élargir la portée de ce type de réglementation au-delà du secteur des télécommunications», a déclaré le Professeur Udo Helmbrecht, [Directeur Exécutif de l'ENISA](#).

La directive sur la déclaration des incidents oriente les NRA vers deux types différents de déclaration des incidents mentionnés dans l'Article 13a: la déclaration résumée annuelle des incidents graves à l'ENISA et à la CE, et la notification ad hoc des incidents aux autres NRA, dans les cas d'incidents transfrontaliers. Cette directive

13/12/2011

www.enisa.europa.eu

définit le champ de la déclaration des incidents, les paramètres des incidents et les seuils. Elle contient également un modèle de déclaration pour soumettre les déclarations des incidents à l'ENISA et à la CE, et explique comment les déclarations seront traitées par l'ENISA. La directive sur les mesures de sécurité minimales conseille aux NRA les mesures de sécurité minimales que les opérateurs de télécommunication devraient prendre pour garantir la sécurité de ces réseaux.

Pour consulter les rapports complets:

[Technical Guideline on Minimum Security Measures](#)

[Technical Guideline on Incident Reporting](#)

Pour toute demande d'interview, veuillez contacter: Ulf Bergstrom, Porte-parole de l'ENISA, press@enisa.europa.eu, Portable: + 30-6948-460-143, ou Dr Marnix Dekker, Expert, Marnix.Dekker@enisa.europa.eu

Veuillez noter : traduction. La version anglaise est la seule version officielle
Veuillez noter: traduction. La version anglaise est la seule version officielle.

www.enisa.europa.eu/media/enisa-en-francais/
www.enisa.europa.eu